UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

CODY LAPERTCHE, Individually, and on behalf of all others similarly situated	§	**CASE NO.**
Plaintiff,	§	**JURY TRIAL DEMANDED**
v.	§	
MR. COOPER GROUP, INC.	§	
Defendant.	§	

CLASS ACTION COMPLAINT

Plaintiff Cody LaPertche, on behalf of himself and all others similarly situated, bring this Class Action Complaint ("Complaint") against Defendant Mr. Cooper Group, Inc., ("Mr. Cooper" or "Defendant") and alleges, upon personal knowledge as to their own actions and their counsel's investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE CASE

1. Plaintiff brings this class action against Defendant for its failure to exercise reasonable care in securing and safeguarding individuals' sensitive personal data (collectively known as "Private Information").

2. On or around October 31, 2023, third-party cyber criminals gained unauthorized access to Plaintiff's and Class members' Private Information (the "Data Breach").

3. The total number of individuals who have had their data exposed due to Defendant's failure to implement appropriate security safeguards is unknown at this time but up to 4,000,000

individuals can be considered at risk.[1]

4. Defendant's security failures enabled the hackers to steal the Private Information of Plaintiff and members of the Class (defined below). These failures put Plaintiff's and Class members' Private Information and interests at serious, immediate, and ongoing risk and, additionally, caused costs and expenses to Plaintiff and Class members associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including, as appropriate, reviewing records for fraudulent charges, cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, initiating and monitoring credit freezes, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach.

5. The Data Breach was caused and enabled by Defendant's violation of its obligations to abide by best practices, industry standards, and federal and state laws concerning the security of individuals' Private Information. Defendant knew or should have known that its failure to take reasonable security measures— which could have prevented or mitigated the Data Breach that occurred— left its customers' Private Information vulnerable to identity theft, financial loss, and other associated harms.

6. Accordingly, Plaintiff asserts claims for negligence, breach of implied contract, breach of the implied covenant of good faith and fair dealing, unjust enrichment/quasi-contract, and breach of confidence.

7. Plaintiff also seeks injunctive relief, monetary damages, statutory damages, and all

---

[1] https://www.nytimes.com/2023/11/07/business/cyberattack-mr-cooper-mortgages.html (last accessed November 9, 2023)

other relief as authorized in equity or by law.

PARTIES

A. PLAINTIFF CODY LAPERTCHE

8. Plaintiff Cody LaPertche is a resident and citizen of California, and brings this action in his individual capacity and on behalf of all others similarly situated.

9. Defendant collected, maintained, and controlled Plaintiff's Private Information in the course of servicing Plaintiff's home loan.

10. Plaintiff received a notice, dated November 2, 2023, from Defendant via electronic mail notifying him of the Data Breach.

11. In maintaining Plaintiff's Private Information, Defendant expressly and impliedly promised to safeguard it. Defendant, however, did not implement proper, industry-standard safeguards to protect Plaintiff's Private Information, leading to its exposure and exfiltration by cybercriminals, who stole the Private Information at issue with the intent to sell it and/or fraudulently misuse it for their own gain.

12. Plaintiff and Class members have faced and will continue to face a certainly impending and substantial risk of future harms because of Defendant's ineffective data security measures, as further set forth herein.

13. Plaintiff LaPertche greatly values his privacy and would not have chosen to do business with Defendant if he had known Defendant would negligently maintain his Private Information as it did.

14. Plaintiff LaPertche has been notified that his phone number was listed on the dark web. Plaintiff has also received multiple cryptic text messages from unfamiliar numbers after the Data Breach.

B. DEFENDANT

15. Defendant Mr. Cooper Group, Inc. is a Texas Limited Liability Corporation with its principal place of business at 8950 Cypress Waters Boulevard, Avenue, Coppell, TX 75019. Its corporate policies, including those on data privacy, are established in and emanate from the State of Texas.

16. Defendant is one of the nation's largest non-bank mortgage servicers.

JURISDICTION AND VENUE

17. The Court has jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2) ("CAFA"), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

18. The Court has personal jurisdiction over Defendant because its principal place of business is located, and they conduct substantial business, in this District.

19. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) because Defendant maintains its principal place of business in this District and therefore reside in this District pursuant to 28 U.S.C. § 1391(c)(2). A substantial part of the events or omissions giving rise to the Class's claims also occurred in this District.

FACTUAL ALLEGATIONS

20. Plaintiff and Class members were Defendant's customers. When customers use Defendant's services, Defendant collects their highly confidential Private Information.

21. On or around November 2, 2023, Defendant began issuing Notice Letters by electronic mail to Plaintiffs and Class members, alerting them that their sensitive Private Information had been exposed in a Data Breach.

22. The Data Breach occurred because Mr. Cooper failed to take reasonable measures to protect the Private Information it collected and stored. Among other things, Defendant failed to implement data security measures designed to prevent this attack, despite repeated warnings about the risk of cyberattacks and the highly publicized occurrence of many similar attacks in the recent past on

other loan servicing platforms.

23. Defendant disregarded the rights of Plaintiff and Class members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff and Class members' Private Information was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data. As a result, the Private Information of Plaintiff and Class members was exfiltrated through unauthorized access by an unknown, malicious cyber hacker with the intent to fraudulently misuse it. Plaintiff and Class members have a continuing interest in ensuring that their compromised Information is and remains safe.

A. DEFENDANT FAILED TO COMPLY WITH INDUSTRY STANDARDS AND FEDERAL AND STATE LAW

24. As a condition of servicing home loans, Defendant is entrusted with the highly confidential Private Information of millions of customers, including Plaintiff and Class members.

25. By obtaining, collecting, using, and deriving a benefit from Plaintiff and Class members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff and Class members' Private Information from disclosure.

26. Defendant had obligations created by industry standards and federal and state law to keep Class members' Private Information confidential and to protect it from unauthorized access and disclosure.

27. Plaintiff and Class members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligation to keep such information confidential and secure from unauthorized access.

28. Defendant's failure to provide adequate security measures to safeguard Plaintiff's and Class members' Private Information is especially egregious because Defendant operates in a field which has recently been a frequent target of scammers attempting to fraudulently gain access to customers' Private Information. Cyber security professionals have consistently identified loan servicing platforms as particularly vulnerable to data breaches because of the value of the Private

Information they collect and maintain.

29. The number of US data breaches surpassed 1,800 in 2021, a record high and a sixty-eight percent increase in the number of data breaches from the previous year.[2]

30. In August 2022, the Consumer Finance Protection Bureau (CFPB) published a circular on data security. The CFPB noted that "[w]idespread data breaches and cyberattacks have resulted in significant harms to consumers, including monetary loss, identity theft, significant time and money spent dealing with the impacts of the breach, and other forms of financial distress," and the circular concluded that the provision of insufficient security for consumers' data can violate the prohibition on "unfair acts or practices" in the Consumer Finance Protection Act (CFPA).[3]

31. Charged with handling sensitive Private Information, Defendant knew, or should have known, the importance of safeguarding its customers' Private Information that was entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on its customers after a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

32. Despite the abundance and availability of information regarding cybersecurity best practices for the loan servicing industry, Defendant chose to ignore them. These best practices were known, or should have been known by Defendant, whose failure to heed and properly implement them directly led to the Data Breach and the unlawful exposure of Private Information.

33. At a minimum, industry best practices should have been implemented by Defendant, including but not limited to requiring customers to create strong passwords; implementing multi-layer security including firewalls and anti-malware software; encrypting data and making it unreadable without a key; updating and patching all systems with the latest security software; and better educating

---

[2] Identity Theft Resource Center, *2021 Annual Data Breach Year-End Review*, https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/

[3] CONSUMER FIN. PROT. BUREAU, *Consumer Financial Protection Circular 2022-04: Insufficient data protection or security for sensitive consumer information* (Aug. 11, 2022), https://files.consumerfinance.gov/f/documents/cfpb_2022-04_circular_2022-08.pdf.

its employees about safe data security practices.

34. Defendant was also on notice that under the FTC Act, Defendant is prohibited from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.[4]

35. Defendant is further required by the comprehensive data privacy regimes enacted by at least 13 states to protect Plaintiff's and Class Members' Private Information, and further, to handle any breach of the same in accordance with applicable breach notification statutes.[5]

36. The potential for improper disclosure of Plaintiff and Class members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take reasonable steps necessary to secure the Private Information from those risks left the Private Information in a vulnerable position.

B. DEFENDANT EXPOSED ITS CUSTOMERS TO IDENTIFY THEFT, FINANCIAL LOSS, AND OTHER HARMS

37. Plaintiff and Class members have been injured by the disclosure of their Private Information in the Data Breach.

38. The fact that Plaintiff and Class members' Private Information was stolen means that Class members' information is likely for sale by cybercriminals and will be misused in additional instances in the future.

39. Private Information is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify

---

[4] *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

[5] International Association of Privacy Professionals, *Delaware Governor Signs Personal Data Privacy Act* (Sep. 12, 2023), https://iapp.org/news/a/delaware-governor-signs-personal-data-privacy-act.

theft and financial fraud.[6] Indeed, a robust "cyber black market" exists in which criminals openly post stolen Private Information on multiple underground Internet websites, commonly referred to as the dark web.

40. The value of Plaintiff and Class members' Private Information on the black market is substantial. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349.[7]

41. Indeed, several news outlets have reported that Plaintiff's and the Class members' data including full names, gender, birth years, and additional genetic data is already for sale on the black market.[8]

42. The FTC has also recognized that consumer data is a valuable form of currency. In an FTC roundtable presentation, a former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[9]

43. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information.[10] The idea is to give consumers more power and control over the type of information that they share and who ultimately

---

[6] Federal Trade Commission, *Warning Signs of Identity Theft* (Sept. 2018), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft .

[7] *See* U.S. Dep't of Justice, *Victims of Identity Theft,* OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

[8] https://www.pelhamplus.com/us-news/stolen-user-data-from-23andme-users-emerges-on-breachform/ (last accessed October 27, 2023)

[9] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMM'N (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

[10] *Web's Hot New Commodity*, *supra* note 17.

receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

44. The ramifications of Defendant's failure to keep its customers' Private Information secure are long-lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to twelve months or even longer.

45. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the Private Information it maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud.

46. Had Defendant remedied the deficiencies in its security systems after the earlier breach, followed industry guidelines, and adopted security measures recommended by experts in the field, Defendant would have prevented the breach of its systems and, ultimately, the theft of its customers' Private Information.

47. The compromised Private Information in the Data Breach is of great value to hackers and thieves and can be used in a variety of ways. Information about an individual that can be logically associated with other information can be chained together, increasing its utility to criminals.

48. In addition, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

49. In short, the Private Information exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breach can be used in a variety of unlawful manners, including opening new credit and financial accounts in users' names.

C. PLAINTIFF AND CLASS MEMBERS SUFFERED DAMAGES FROM THE DATA BREACH

50. Plaintiff and the Class have been damaged by the compromise of their Private Information in the Data Breach.

51. The ramifications of Defendant's failure to keep its customers' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that

information and damage to the victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[11]

52. In addition to its obligations under state and federal laws and regulations, Defendant owed a common law duty to Plaintiff and Class members to protect the Private Information they entrusted to it, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized parties.

53. Defendant further owed and breached its duty to Plaintiff and Class members to implement processes and specifications that would detect a breach of its security systems in a timely manner and to act upon warnings and alerts, including those generated by its own security systems.

54. As a direct result of Defendant's intentional, willful, reckless, and negligent conduct which resulted in the Data Breach, unauthorized parties were able to access, acquire, view, publicize, and/or otherwise commit the identity theft and misuse of Plaintiff and Class members' Private Information as detailed above, and Plaintiff and members of the Class are at a heightened and increased substantial risk of suffering identity theft and fraud.

55. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds to thousands of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

56. Some of the injuries and risks associated with the loss of personal information have already manifested themselves in Plaintiff and other Class members' lives. Each Plaintiff received a cryptically written notice letter from Defendant stating that their Private Information was released, and that they should remain vigilant for fraudulent activity, with no other explanation of where this

---

[11] *2014 LexisNexis True Cost of Fraud Study*, LEXISNEXIS (Aug. 2014), https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

Information could have gone, or who might have access to it.

57. Plaintiff and the Class face a substantial risk of suffering out-of-pocket fraud losses such as fraudulent charges on online accounts, credit card fraud, applications for benefits made fraudulently in their names, loans opened in their names, medical services billed in their names, government benefits fraudulently drawn in their name, and identity theft. Many Class members may already be victims of identity theft and fraud without realizing it.

58. Plaintiff and Class members have, may have, and/or will have incurred out of pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

59. Plaintiff and Class members would not have obtained services from Defendant had they known that Defendant failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their Private Information from criminal theft and misuse.

60. Plaintiff and the Class will continue to spend significant amounts of time to monitor their financial accounts for misuse.

61. Identity thieves can use the victim's Private Information to commit any number of frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest. As a result, Plaintiff and Class members now face a real and continuing immediate risk of identity theft and other problems associated with the disclosure of their Social Security numbers and will need to monitor their credit for an indefinite duration. For Plaintiff and Class members, this risk creates unending feelings of fear and annoyance. Private information is especially valuable to identity thieves. Defendant knew or should have known this and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

62. As a result of the Data Breach, Plaintiff and Class members' Private Information has diminished in value.

63. The Private Information belonging to Plaintiff and Class members is private and was left inadequately protected by Defendant who did not obtain Plaintiff or Class members' consent to

disclose such Private Information to any other person as required by applicable law and industry standards. Defendant disclosed Plaintiff and Class members' Private Information as a direct result of its inadequate security measures.

64. The Data Breach was a direct and proximate result of Defendant's failure to: (a) properly safeguard and protect Plaintiff and Class members' Private Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff and Class members' Private Information; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

65. Defendant had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite its obligation to protect customer data.

66. Defendant did not properly train its employees, particularly its information technology department, to timely identify cyber attacks and other data security risks.

67. Had Defendant remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field, it would have prevented the intrusions into its systems and, ultimately, the theft of Plaintiff and Class members' Private Information.

68. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

69. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, twenty-nine percent spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could]

take more than a year for some victims."[12]

70. Other than offering 12 months of credit monitoring, Defendant did not take any measures to assist Plaintiff and Class members.

71. The limited offer of credit monitoring is woefully inadequate. While some harm has already taken place, the worst is yet to come. There may be a time lag between when harm occurs versus when it is discovered, and between when Private Information is acquired and when it is used. Furthermore, identity theft monitoring only alerts someone to the fact that they have already been the victim of identity theft (*i.e.*, fraudulent acquisition and use of another person's Private Information) – it does not prevent identity theft.[13]

72. Defendant's failure to adequately protect Plaintiff and Class members' Private Information has resulted in Plaintiff and Class members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money–while Defendant sits by and does nothing to assist those affected by the incident. Instead, as Defendant's notice confirms, the burden is on Plaintiff and Class members to discover possible fraudulent activity and identity theft and mitigate the negative impacts arising from such fraudulent activity on their own.

73. Plaintiff and Class members have been damaged in several other ways as well. Plaintiff and Class members have been exposed to an impending, imminent, and ongoing increased risk of fraud, identity theft, and other misuse of their Private Information. Plaintiff and Class members must now and indefinitely closely monitor their financial and other accounts to guard against fraud. This is a burdensome and time-consuming task. Class members have also been forced to purchase adequate credit reports, credit monitoring and other identity protection services, and have placed credit freezes

---

[12] *See* U.S. Dep't of Justice, *Victims of Identity Theft,* OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

[13] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, CNBC (Nov. 30, 2017), https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-beworth-the-cost.html.

and fraud alerts on their credit reports, while also spending significant time investigating and disputing fraudulent or suspicious activity on their accounts. Plaintiff and Class members also suffered a loss of the inherent value of their Private Information.

74. The Private Information stolen in the Data Breach can be misused on its own or can be combined with personal information from other sources such as publicly available information, social media, etc. to create a package of information capable of being used to commit further identity theft. Thieves can also use the stolen Private Information to send spear-phishing emails to Class members to trick them into revealing sensitive information. Lulled by a false sense of trust and familiarity from a seemingly valid sender (for example Wells Fargo, Amazon, or a government entity), the individual agrees to provide sensitive information requested in the email, such as login credentials, account numbers, and the like.

75. As a result of Defendant's failures to prevent the Data Breach, Plaintiff and Class members have suffered, will suffer, and are at increased risk of suffering:

- The compromise, publication, theft and/or unauthorized use of their Private Information;
- Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;
- Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;
- The continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the Private Information in its possession;
- Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class members; and

- Anxiety and distress resulting fear of misuse of their Private Information.

76. In addition to a remedy for the economic harm, Plaintiff and Class members maintain an undeniable interest in ensuring that their Private Information remains secure and is not subject to further misappropriation and theft.

CLASS ACTION ALLEGATIONS

116. Plaintiff brings all counts, as set forth below, individually and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure, on behalf of a "Nationwide Class" (the "Class") defined as:

Nationwide Class

All persons who submitted their Private Information to Defendant and whose Private Information was compromised as a result of the data breach(es) discovered in or about October 2023.

117. Excluded from the Class are Defendant and Defendant's affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

118. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

119. **Numerosity**—Federal Rule of Civil Procedure 23(a)(1). The members of the Class are so numerous that joinder of all Class members would be impracticable. On information and belief, the Class has thousands of members.

120. **Commonality and Predominance**—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3). Common questions of law and fact exist as to all members of the Class and predominate over questions affecting only individual members of the Class. Such common questions of law or fact

include, inter alia:

a. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, e.g., FTCA (as discussed below);

b. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

c. Whether Defendant properly implemented their purported security measures to protect Plaintiff's and the Class's Private Information from unauthorized capture, dissemination, and misuse;

d. Whether Defendant took reasonable measures to determine the extent of the Data Breach after they first learned of same;

e. Whether Defendant disclosed Plaintiff's and the Class's Private Information in violation of the understanding that the Private Information was being disclosed in confidence and should be maintained;

f. Whether Defendant's conduct constitutes breach of an implied contract;

g. Whether Defendant willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and the Class's Private Information;

h. Whether Defendant were negligent in failing to properly secure and protect Plaintiff's and the Class's Private Information;

i. Whether Defendant was unjustly enriched by its actions; and

j. Whether Plaintiff and the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

121. Defendant engaged in a common course of conduct giving rise to the legal rights

sought to be enforced by Plaintiff, on behalf of herself and other members of the Class. Similar or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

122. **Typicality**—Federal Rule of Civil Procedure 23(a)(3). Plaintiff's claims are typical of the claims of the other members of the Class because, among other things, all Class members were similarly injured through Defendant's uniform misconduct described above and were thus all subject to the Data Breach alleged herein. Further, there are no defenses available to Defendant that are unique to Plaintiff.

123. **Adequacy of Representation**—Federal Rule of Civil Procedure 23(a)(4). Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the Class he seeks to represent, he has retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiff and her counsel.

124. **Injunctive Relief**—Federal Rule of Civil Procedure 23(b)(2). Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2).

125. **Superiority**—Federal Rule of Civil Procedure 23(b)(3). A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the Class are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for members of the Class to individually seek redress for Defendant's wrongful conduct. Even if members of the Class could afford individual litigation, the court system could not.

Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSE OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of the Nationwide Class, or, Alternatively, the California Subclass)

126. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

127. Upon Defendant's accepting and storing the Private Information of Plaintiff and the Class in its computer systems and on its networks, Defendant undertook and owed a duty to Plaintiff and the Class to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendant knew that the Private Information was private and confidential and should be protected as private and confidential.

128. Defendant owed a duty of care not to subject Plaintiff's and Class members' Private Information to an unreasonable risk of exposure and theft because Plaintiff and Class members were foreseeable and probable victims of any inadequate security practices.

129. Defendant owed numerous duties to Plaintiff and the Class, including the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information in its possession;

b. to protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

130. Defendant also breached its duty to Plaintiff and Class members to adequately protect and safeguard Private Information by disregarding standard information security principles, despite

obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information. Furthering its dilatory practices, Defendant failed to provide adequate supervision and oversight of the Private Information with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a malicious third party to gather Plaintiff's and Class members' Private Information and potentially misuse it and intentionally disclose it to others without consent.

131. Defendant knew, or should have known, of the risks inherent in collecting and storing Private Information and the importance of adequate security.

132. Defendant knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiff's and Class members' Private Information.

133. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class members from a data breach.

134. Defendant breached its duties to Plaintiff and Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information.

135. Because Defendant knew that a breach of its systems would damage at least a million of its customers, including Plaintiff and Class members, Defendant had a duty to adequately protect its data systems and the Private Information contained thereon.

136. Defendant's duty of care to use reasonable security measures arose from of the special relationship that existed between Defendant and its customers, which is recognized by data privacy laws and regulations under the laws of 13 states.

137. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

138. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant are bound by industry standards to protect confidential Private Information.

139. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their Private Information. Defendant's misconduct included failing to: (1) secure Plaintiff's and Class members' Private Information; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

140. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class members' Private Information;

b. Failing to adequately monitor the security of Defendant's networks and systems;

c. Allowing unauthorized access to Class members' Private Information;

d. Failing to detect in a timely manner that Class members' Private Information had been compromised; and

141. Through Defendant's acts and omissions described in this Complaint, including its failure to provide adequate security and its failure to protect Plaintiff's and Class members' Private Information from being foreseeably captured, accessed, disseminated, stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff's and Class members' Private Information during the time it was within Defendant's possession or control.

142. Defendant's conduct was grossly negligent and departed from all reasonable standards of care.

143. Neither Plaintiff nor the other Class members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

144. As a direct and proximate cause of Defendant's conduct, Plaintiff and Class members suffered damages as alleged above.

145. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide lifetime free

credit monitoring to all Class members.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of the Nationwide Class, or, Alternatively, the California Subclass)

146. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

147. Defendant acquired the Private Information of Plaintiff and Class members when it serviced their loans as part of Defendant's regular business practices.

148. In so doing, Plaintiff and Class members entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such information and to timely detect any breaches of their Private Information. In entering into such implied contracts, Plaintiff and Class members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including the FTCA, and were consistent with industry standards.

149. Plaintiff and Class members would not have provided and entrusted their Private Information with Defendant in the absence of the implied contract between them and Defendant.

150. Plaintiff and Class members fully performed their obligations under the implied contracts with Defendant.

151. Defendant breached the implied contracts they made with Plaintiff and Class members by failing to safeguard and protect their Private Information and by failing to timely detect the Data Breach within a reasonable time.

152. As a direct and proximate result of Defendant's breaches of the implied contracts between Defendant, Plaintiff and Class members, Plaintiff and Class members sustained actual losses and damages as described in detail above.

153. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide free credit monitoring to all Class members.

COUNT III
BREACH OF THE IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING
(On Behalf of the Nationwide Class)

154. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

155. Plaintiff and Class members entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such information and to timely detect any breaches of their Private Information.

156. Plaintiff and Class members would not have provided and entrusted their Private Information with Defendant in the absence of the implied contract between them and Defendant.

157. Every contract has an implied covenant of good faith and fair dealing, which imposes an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

158. Plaintiff and Class members fully performed their obligations under the implied contracts with Defendant.

159. Defendant breached the implied covenant of good faith and fair dealing they made with Plaintiff and Class members by failing to maintain adequate computer systems and data security practices to safeguard and protect their Private Information; failing to timely and accurately disclose the Data Breach to Plaintiff and the Class members; and by continuing to collect and store Plaintiff's and Class members' Private Information after Defendant knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach,

160. Defendant acted in bad faith and/or with malicious motive in denying Plaintiff and Class members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to determined at trial.

COUNT IV
UNJUST ENRICHMENT/QUASI-CONTRACT
(On Behalf of the Nationwide Class)

161. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set

forth herein.

162. Plaintiff and Class members conferred monetary benefits on Defendant by providing Defendant with their Private Information.

163. In exchange, Plaintiff and Class members should have received from Defendant the loan servicing that was the subject of the transaction and should have been entitled to have Defendant protect their Private Information with adequate data security.

164. Defendant knew that Plaintiff and Class members conferred a benefit on it and accepted and has retained that benefit. Defendant profited from servicing Plaintiff and Class members' loans and used Plaintiff's and Class members' Private Information for its regular business purposes.

165. Defendant failed to secure Plaintiff's and Class members' Private Information and, therefore, did not provide full compensation for the benefit the Plaintiff's and Class members' payments and Private Information provided.

166. Defendant acquired the Private Information through inequitable means as it failed to disclose the inadequate security practices previously alleged.

167. If Plaintiff and Class members knew that Defendant would not secure their Private Information using adequate security, they would not have paid for Defendant's services, nor entrusted Defendant with their Private Information.

168. Plaintiff and Class members have no adequate remedy at law.

169. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class members conferred on it.

170. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class members overpaid.

COUNT V
BREACH OF CONFIDENCE
(On Behalf of the Nationwide Class, or, Alternatively, the California Subclass)

94. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set

forth herein.

95. Plaintiff and Class members have an interest, both equitable and legal, in the Private Information that was conveyed to and collected, stored, and maintained by Defendant and which was ultimately compromised by unauthorized cybercriminals as a result of the Data Breach.

96. Defendant, in taking possession of this highly sensitive information, has a special relationship with its customers, including Plaintiff and the Class. As a result of that special relationship, Defendant was provided with and stored private and valuable information belonging to Plaintiff and the Class, which Defendant was required by law and industry standards to maintain in confidence.

97. Plaintiff and the Class provided such Private Information to Defendant under both the express and/or implied agreement of Defendant to limit and/or restrict completely the use and disclosure of such Private Information without Plaintiff's and Class members' consent.

98. Defendant had a common law duty to maintain the confidentiality of Plaintiff's and Class members' Private Information.

99. Defendant owed a duty to Plaintiff and Class members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Private Information in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

100. As a result of the parties' relationship of trust, Defendant had possession and knowledge of the confidential Private Information of Plaintiff and Class members.

101. Plaintiff's and Class members' Private Information is not generally known to the public and is confidential by nature. Moreover, Plaintiff and Class members did not consent to nor authorize Defendant to release or disclose their Private Information to unknown criminal actors.

102. Defendant breached the duty of confidence it owed to Plaintiff and Class members when Plaintiff's and Class members' Private Information was disclosed to unknown criminal hackers

by way of Defendant's own acts and omissions, as alleged herein.

103. Defendant knowingly breached its duties of confidence by failing to safeguard Plaintiff's and Class members' Private Information, including by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of the Private Information; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the Data Breach at the time it began or within a reasonable time thereafter and give adequate notice to Plaintiff and Class members thereof; (g) failing to follow its own privacy policies and practices published to its customers; (h) storing Private Information in an unencrypted and vulnerable manner, allowing its disclosure to hackers; and (i) making an unauthorized and unjustified disclosure and release of Plaintiff's and Class members' Private Information to a criminal third party.

104. But for Defendant's wrongful breach of confidence owed to Plaintiff and Class members, their privacy would not have been compromised and their Private Information would not have been accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by and/or viewed by unauthorized third parties.

105. As a direct and proximate result of Defendant's breach of confidence, Plaintiff and Class members have suffered or will suffer injuries, including but not limited to, the following: loss of their privacy and confidentiality in their Private Information; theft of their Private Information; costs associated with the detection and prevention of fraud and unauthorized use of their Private Information; costs associated with purchasing credit monitoring and identity theft protection services;

costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Defendant's Data Breach – including finding fraudulent charges, enrolling in credit monitoring and identity theft protection services, and filing reports with the police and FBI; the imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals; damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class members' data against theft and not allow access and misuse of their data by others; continued risk of exposure to hackers and thieves of their Private Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' data; and/or mental anguish accompanying the loss of confidence and disclosure of their confidential Private Information.

106. Defendant breached the confidence of Plaintiff and Class members when it made an unauthorized release and disclosure of their confidential Private Information and, accordingly, it would be inequitable for Defendant to retain the benefits it has received at Plaintiff's and Class members' expense.

107. As a direct and proximate result of Defendant's breach of confidence, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

COUNT VI
INJUNCTIVE/DECLARATORY RELIEF
(On Behalf of the Nationwide Class)

108. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

109. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. The Court also has broad authority to restrain acts, such as here, that are tortious and violate the terms of the regulations described in this Complaint.

110. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective duties to reasonably safeguard users' Private Information and whether Defendant is maintaining data security measures adequate to protect the Class members, including Plaintiff, from further data breaches that compromise their Private Information.

111. Plaintiff alleges that Defendant's data-security measures remain inadequate. In addition, Plaintiff and the Class continue to suffer injury as a result of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information and fraudulent activity against them will occur in the future.

112. Pursuant to its authority under the Declaratory Judgment Act, Plaintiff asks the Court to enter a judgment declaring, among other things, the following: (i) Defendant owes a duty to secure customers' Private Information and to timely notify consumers of a data breach under the common law and various federal and state statutes; and (ii) Defendant is in breach of these legal duties by failing to employ reasonable measures to secure customers' Private Information in its possession and control.

113. Plaintiff further asks the Court to issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect customers' Private Information from future data breaches.

114. If an injunction is not issued, the Class members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, the Class members will not have an adequate remedy at law because many of the resulting injuries would not be readily

quantifiable and Class members will be forced to bring multiple lawsuits to rectify the same misconduct.

115. The hardship to the Class members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if a similar data breach occurs again due to the repeated misconduct of Defendant, the Class members will likely be subjected to substantial hacking and phishing attempts, fraud, and other instances of the misuse of their Private Information, in addition to the damages already suffered. On the other hand, the cost to Defendant of complying with an injunction by employing better and more reasonable prospective data security measures is relatively minimal, and Defendant has pre-existing legal obligations to employ such measures.

116. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing additional data breaches at Defendant, thus eliminating the additional injuries that would result to the Class members and the individuals whose personal and confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a. For an order certifying the proposed classes and appointing Plaintiff and her counsel to represent the Class;

b. For an order awarding Plaintiff and Class members actual, statutory, punitive, and/or any other form of damages provided by and pursuant to the statutes cited above;

c. For an order awarding Plaintiff and Class members restitution, disgorgement and/or other equitable relief provided by and pursuant to the statutes cited above or as the Court deems proper;

d. For an order or orders requiring Defendant to adequately remediate the Breach and its effects.

e. For an order awarding Plaintiff and Class members pre-judgment and post-judgment interest;

f. For an order awarding Plaintiff and the Class members reasonable attorneys' fees and costs of suit, including expert witness fees;

g. For an order awarding such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all claims so triable.

Dated: November 14, 2023

Respectfully submitted,

By: */s/Michael A. Josephson*

Michael A. Josephson
Texas Bar No. 24014780
Andrew W. Dunlap
Texas Bar No. 24078444
JOSEPHSON DUNLAP, LLP
11 Greenway Plaza, Suite 3050
Houston, Texas 77046
713-352-1100 – Telephone
713-352-3300 – Facsimile
mjosephson@mybackwages.com
adunlap@mybackwages.com

Nicholas A. Migliaccio*
Jason S. Rathod*
MIGLIACCIO & RATHOD, LLP
412 H Street NE, no. 302,
Washington, DC, 20002
202-470-3520 – Telephone
nmigliaccio@classlawdc.com
jrathod@classlawdc.com

* *pro hac vice* forthcoming

Attorneys for Plaintiff and the Proposed Class